Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Amended Claims:

1. (Currently amended) A system for secure communication across a communication network comprising:

a personal code generation means having ~~one or more~~ an identification ~~codes~~ code and ~~one or more~~ an encryption ~~codes~~ code, ~~each~~ the identification code and ~~each~~ the encryption code being arranged to change randomly at predetermined intervals of ~~with~~ time; and

a code server including ~~each~~ the identification code and ~~each~~ the encryption code, the code server being synchronised with the personal code generation means such that ~~each~~ the identification code of the code server and ~~each~~ the encryption code of the code server change independently of and in synchronisation with ~~each~~ the identification code of the personal code generation means and ~~each~~ the encryption code of the personal code generation means respectively, such that the code server is able to independently determine the identification code and the encryption code of the personal code generation means at any instant of time;

wherein, in use, a user transmits across the communication network, ~~each~~ only the identification code of the personal code generation means ~~and~~ together with data encrypted with ~~each~~ the current encryption code of the personal code generation means and wherein the code server ~~uses each~~ matches the identification code of the personal code

generation means with the corresponding identification code of the code server to authenticate the user and ~~each~~ uses the corresponding encryption code ~~of~~ in the code server to decrypt the transmitted data.

2. (Currently amended) A system for secure communication in accordance with claim 1, wherein the code server communicates to the user following authentication of the user by transmitting data across the communication network to the user encrypted with ~~each~~ the encryption code of the code server and the user decrypts the data transmitted by the code server with ~~each~~ the encryption code of the personal code generation means.

3. (Currently amended) A system for secure communication in accordance with claim 1, wherein the code server stores information including a username assigned to the owner of the personal code generation means and the username is transmitted across the communication network with ~~each~~ the identification code of the personal code generation means and the data encrypted with ~~each~~ the encryption code of the personal code generation means and the code server uses the username to authenticate the user as the owner of the personal code generation means.

4. (Currently amended) A system for secure communication in accordance with claim 1, wherein the code server stores information including a password assigned to the owner of the personal code generation means and the password is transmitted across the communication network with ~~each~~ the identification

code of the personal code generation means and the data encrypted with ~~each~~ the encryption code of the personal code generation means and the code server uses the password to authenticate the user as the owner of the personal code generation means.

5.   (Previously presented) A system for secure communication in accordance with claim 1, wherein the personal code generation means comprises a personal portable token.

6.   (Original) A system for secure communication in accordance with claim 5, wherein the personal portable token is a pendant.

7.   (Original) A system for secure communication in accordance with claim 5, wherein the personal portable token is a card.

8.   (Currently amended) A system for secure communication in accordance with claim 5, wherein the personal code generation means includes a communication port to communicate ~~each~~ the identification code of the personal code generation means and ~~each~~ the current encryption code of the personal code generation means to a user's computer.

9.   (Previously presented) A system for secure communication in accordance with claim 1, wherein the personal code generation means comprises software residing on a user's computer.

10.   (Currently amended) A system for secure communication in accordance with claim 5, wherein the personal code generation means includes a display means, the display means displaying ~~each~~ the identification code of the personal code generation means and ~~each~~ the encryption code of the personal code generation means.

11.   (Currently amended) A system for secure communication in accordance with claim 5, wherein the personal code generation means comprises a smart card having an initialisation code known to the code server and software residing on a user's computer, the software being capable of generating ~~each~~ the identification code and each encryption code based on the initialisation code and a reference clock, the code server also being capable of generating ~~each~~ the identification code and ~~each~~ the encryption code based on the initialisation code and the reference clock.

12. (Currently amended)   A system for securely accessing data stored in an encrypted form on a storage means accessible by a communication network comprising:

a personal code generation means having ~~one or more~~ an identification ~~codes~~ code and ~~one or more~~ an encryption ~~codes~~ code , ~~each~~ the identification and ~~each~~ the encryption code being arranged to change randomly at predetermined intervals of ~~with~~ time;

a key archive associated with the personal code generation means and with one or more data files on the storage means, the key archive having information including

the location of the data files and the encryption codes with which each of the data files is encrypted, the key archive being encrypted with an archiving code; and

a code server including ~~each~~ the identification code and ~~each~~ the encryption code, the code server being synchronised with the personal code generation means such that ~~each~~ the identification code of the code server and ~~each~~ the encryption code of the server change independently of and in synchronisation with ~~each~~ the identification code of the personal code generation means and ~~each~~ the encryption code of the personal code generation means, the code server also having a previous archiving code being the archiving code last used to encrypt the key archive and a current archiving code being arranged to change with time;

wherein when a user wishes to access each stored data file, the user transmits across the communication network, ~~each~~ only the identification code of the personal code generation means and data including a request to access the stored data files encrypted with ~~each~~ the encryption code of the personal code generation means and wherein the code server ~~uses each~~ matches the identification code of the personal code generation means with the corresponding identification code of the code server to authenticate the user and uses the corresponding encryption code of the code server to decrypt the transmitted data and wherein the code server communicates to the user the previous archiving code in encrypted form using ~~each~~ the encryption code ~~of~~ in the code server so that the user may decrypt the key archive providing access to the stored data files.

13.   (Original) A system for securely accessing data stored in accordance with claim 12, wherein when the code server transmits to the user the previous archiving code, the code server also transmits the current archiving code and the user then uses the current archiving code to encrypt the key archive when the user has completed accessing the stored data files and the code server stores the current archiving code as the previous archiving code for future access to the store data files.

14.   (Currently amended) A method for securely communicating across a communication network comprising the steps of:

providing a personal code generation means to a user, the personal code generation means having ~~one or more~~ an identification ~~codes~~ code and ~~one or more~~ an encryption ~~codes~~ code, ~~each~~ the identification code and ~~each~~ the encryption code being arranged to change randomly at predetermined intervals of ~~with~~ time; and

providing a code server including ~~each~~ the identification code and ~~each~~ the encryption code and synchronising the code server with the personal code generation means such that ~~each~~ the identification code of the code server and ~~each~~ the encryption code of the code server change independently of and in synchronisation with ~~each~~ the identification code of the personal code generation means and ~~each~~ the encryption code of the personal code generation means respectively, such that the code server is able to independently determine the identification code and the encryption code of the personal code generation means at any instant of time; and

the user transmitting across the communication network, ~~each~~ only the identification code of the personal code generation means and data encrypted with ~~each~~ the encryption code of the personal code generation means and wherein the code server matches the identification code of the personal code generation means with the corresponding identification code of the code server to authenticate the user and ~~each~~ uses the corresponding encryption code ~~of~~ in the code server to decrypt the transmitted data.

15. (Previously presented) A method for securely communicating across a communication network in accordance with claim 14 further comprising the step of the code server communicating to the user following authentication of the user by transmitting data across the communication network to the user encrypted with the encryption code of the code server and the user decrypting the data transmitted by the code server with the encryption code of the personal code generation means.

16. (Currently amended) A method for securely communicating across a communication network in accordance with claim 14, further comprising the steps of providing the user with a username and password known to the code server and transmitting the username and password across the communication network with ~~each~~ the identification code of the personal code generation means and the data encrypted with ~~each~~ the encryption code of the personal code generation means and the code server using the username and password to

authenticate the user of the personal code generation means.

17. (Previously presented) A method for securely accessing data stored in an encrypted form on a storage means accessible by a communication network comprising the steps of:

providing a personal code generation means having ~~one or more~~ an identification ~~codes~~ code and ~~one or more~~ an encryption ~~codes~~ code, ~~each~~ the identification and ~~each~~ the encryption code being arranged to change randomly at predetermined intervals of ~~with~~ time;

providing a key archive associated with the personal code generation means and with one or more data files on the storage means, the key archive having information including the location of the data files and encryption keys with which each of the data files is encrypted, the key archive being encrypted with an archiving code; and

synchronising the code server with the personal code generation means such that ~~each~~ identification code of the code server and ~~each~~ the encryption code of the code server change independently of and in synchronisation with ~~each~~ the identification code of the personal code generation means and ~~each~~ the encryption code of the personal code generation means respectively, such that the code server is able to independently determine the identification code and the encryption code of the personal code generation means at any instant of time, the code server also having a previous

archiving code being the archiving code last used to encrypt
the key archive and a current archiving code being arranged
to change at predetermined time intervals;

the user transmitting across the communication
network, ~~each~~ only the identification code of the personal
code generation means and data including a request to access
the stored data files encrypted with ~~each~~ the encryption
code of the personal code generation means;

wherein the code server matches the identification code
of the personal code generation means with the corresponding
identification code of the code server to authenticate the
user and ~~each~~ uses the corresponding encryption code ~~of~~ in
the code server to decrypt the transmitted data and wherein
the code server ~~communicating~~ communicates to the user the
previous archiving code in encrypted form so that the user
may decrypt the key archive providing access to the stored
data files.

18. (Previously presented) A method for securely accessing
data stored in an encrypted form on a storage means
accessible by a communication network in accordance with
claim 17, further comprising the steps of:

the user using the current archiving code to encrypt
the key archive on completing accessing the stored data
files; and the code server storing the current archiving
code as the previous archiving code for future access to
the store data files.

19. (New) A system for secure communication in accordance with claim 1, wherein the identification code is one of a plurality of identification codes.

20. (New) A system for secure communication in accordance with claim 1, wherein the encryption code is one of a plurality of encryption codes.

21. (New) A system for securely accessing stored data in accordance with claim 12, wherein the identification code is one of a plurality of identification codes.

22. (New) A system for securely accessing stored data in accordance with claim 12, wherein the encryption code is one of a plurality of encryption codes.

23. (New) A method for securely communicating across a communication network in accordance with claim 14, wherein the identification code is one of a plurality of identification codes.

24. (New) A method for securely communicating across a communication network in accordance with claim 14, wherein the encryption code is one of a plurality of encryption codes.

25. (New) A method for securely accessing data stored in an encrypted form on a storage means accessible by a communication network in accordance with claim 17, wherein the identification code is one of a plurality of identification codes.

26. (New) A method for securely accessing data stored in an encrypted form on a storage means accessible by a communication network in accordance with claim 17, wherein the encryption code is one of a plurality of encryption codes.